

Public Key Infrastructure (PKI) Awareness Training



IA CAC/PAK Division

8 February 2006

AGENDA



Module A:	Overview
Module B:	Army Knowledge Online (AKO)
Module C:	Software Requirements
Module D:	Installing Middleware
Module E:	Installing Card Readers
Module F:	Obtaining and Installing DOD Roots
Module G:	Registering the CAC
Module H:	Configuring the Email Client
Module I:	Using PKI with the CAC
Module J:	Retrieving Other User's Certificates
Module K:	Web Authentication
Module L:	Questions and Comments



Army CAC Program Scope

- Over **1.4 Million CACs** have been issued worldwide to:
 - Active Army personnel
 - Army Guard and Reserve personnel
 - Department of Army Civilian personnel
 - Eligible Army Contractors
- The total could potentially reach **2.5 million CACs** when it is issued to Family Members and Retirees in the future.
- The CAC will **significantly** change the way the Army does business

Guidance on the use of Digital Signature



Sending Digitally Signed Email

- Army Email users should Digitally Sign their Email messages when data integrity or non-repudiation services are required.
- This guidance does not apply to General Officers (GO) or Senior Executive Service (SES) Personnel. Specific guidance for GOs and SESs has been issued by the Chief of Staff of the Army.

Receiving Digitally Signed Email

- Emails signed with revoked certificates should be treated as not having originated from the indicated sender.

****Ref:** HQDA Memorandum, Subject: Army Public Key Infrastructure (PKI) Usage Guidance For Encryption and Digital Signing of E-mail Messages, Dated 03 May 02.

Guidance on the Encryption of Email Messages



Sending Encrypted Email

- Sending Encrypted Email should be the EXCEPTION not the RULE.
- Encryption must use DOD Class 3 Encryption Certificates
- Encrypted Email should be used to send:
 - Information protected by the Privacy Act
 - Information classified as “For Official Use Only” (FOUO)
 - Sensitive but Unclassified Data
 - Information covered under the Health Insurance Portability and Accountability Act (HIPAA)

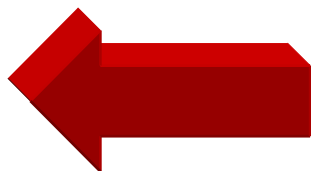
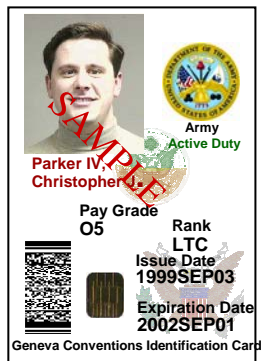
Receiving Encrypted Email

- If a message has been encrypted, the implication is that it contains ***Sensitive but Unclassified Information***.
- Email that is received encrypted should be maintained in encrypted form.

**Ref: HQDA Memorandum, Subject: Army Public Key Infrastructure (PKI) Usage Guidance For Encryption and Digital Signing of E-mail Messages, Dated 03 May 02.

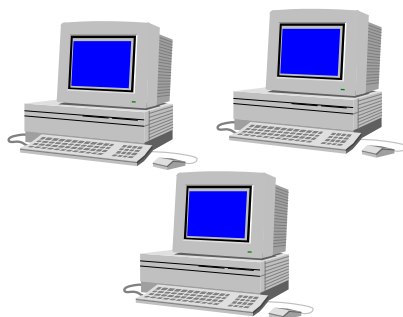
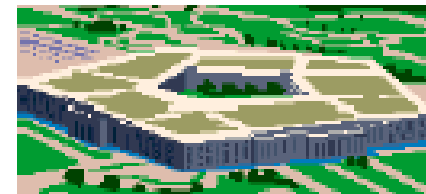


What Does a CAC Do?



Personnel Identification
Replaces the "ID" Card

Building Access



Systems & Network Access
with PKI Application Provides:

- Digital Signature
- Data Encryption

Many Other Functional Applications



Medical, Logistics,
Personnel, Travel,
Acquisition, etc.



Common Access Card Layout

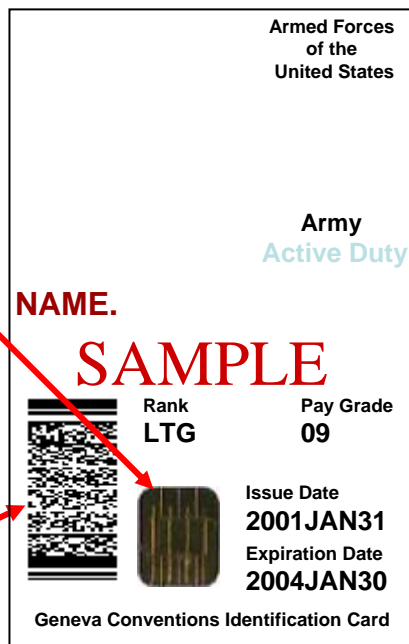
Integrated Circuit Chip Location

- Currently uses 32K Chip.
- **PKI Certificates use 9.9K to 12.9K of Chip space.**
- Future residual space for other functional and service applications.

Barcode for Functional Applications

Current Uses Include:

- Army Food Management Information System (AFMIS) – 3 sites
- USAREUR (Army/USAF) – Motor Vehicle Registration – 26 workstations
- USMC Flightline Access Control System – 8 sites



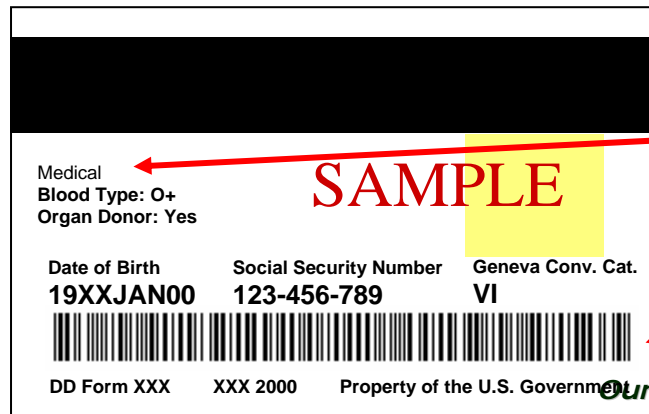
Magnetic Stripe

- Proposed use is for building and facility Access.
- Navy currently uses one track for ATM access

Medical Data

Shows the Blood Type and Organ Donor Status.

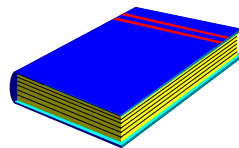
Barcode for Personnel Data





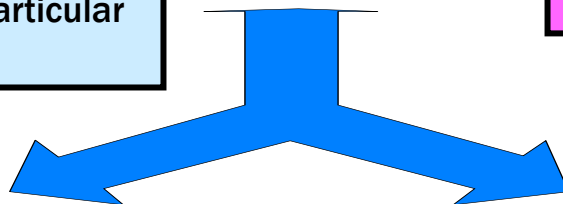
DOD PKI Documentation

DOD X.509 CERTIFICATE POLICY (CP)



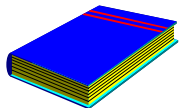
The CP is the unified policy under which a CA operated by a DOD component is established and functions. It does not define a particular implementation of a PKI.

These documents can be found at
<https://iacacpki.army.mil/>

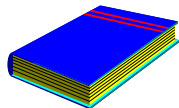


CLASS 3 ASSURANCE CERTIFICATION PRACTICE STATEMENTS (CPS)

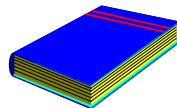
These documents define the specific practices (policies and procedures) under which the US DOD Class 3 PKI will operate. They must meet any requirements of the CP.



Class 3 Root CA
CPS

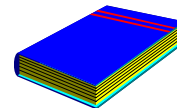


Class 3 Signing
CA CPS



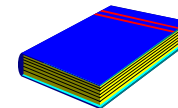
Class 3 RA CPS

- RA SOP
- RA Workstation Settings Doc



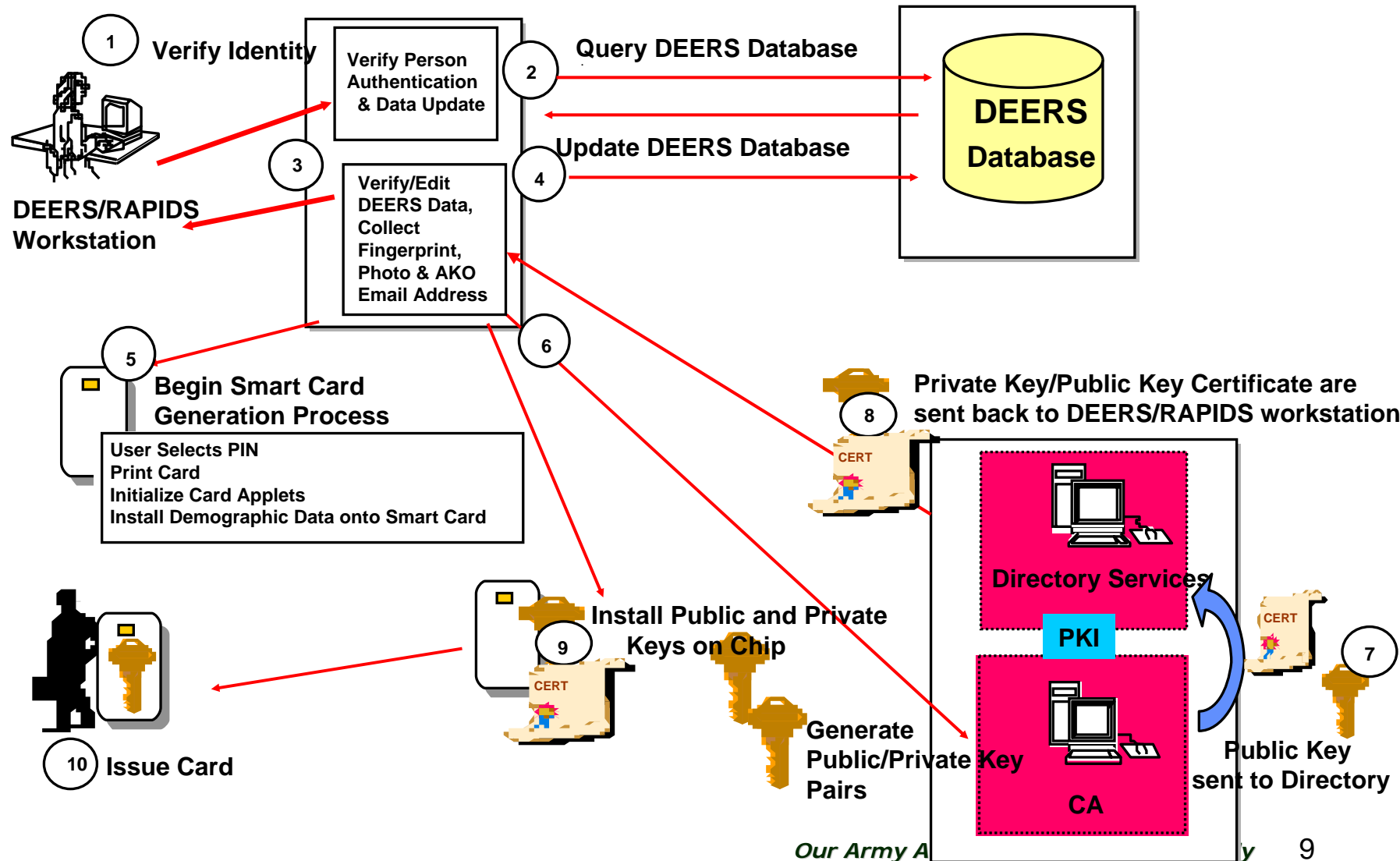
Class 3 LRA CPS

- LRA SOP
- LRA Workstation Settings Doc



Class 3 Key
Recovery CPS

CAC Integrated with PKI





Private and Public Keys

Key pairs generated at the same time

Private Key



- Protected by owner
- Used to sign messages
- Used to decrypt messages
- Kept in physical possession of owner

Public Key







- Distributed freely and openly
- Used to verify signatures
- Used to encrypt messages
- Stored in user's Contacts folder
- Available through the Internet

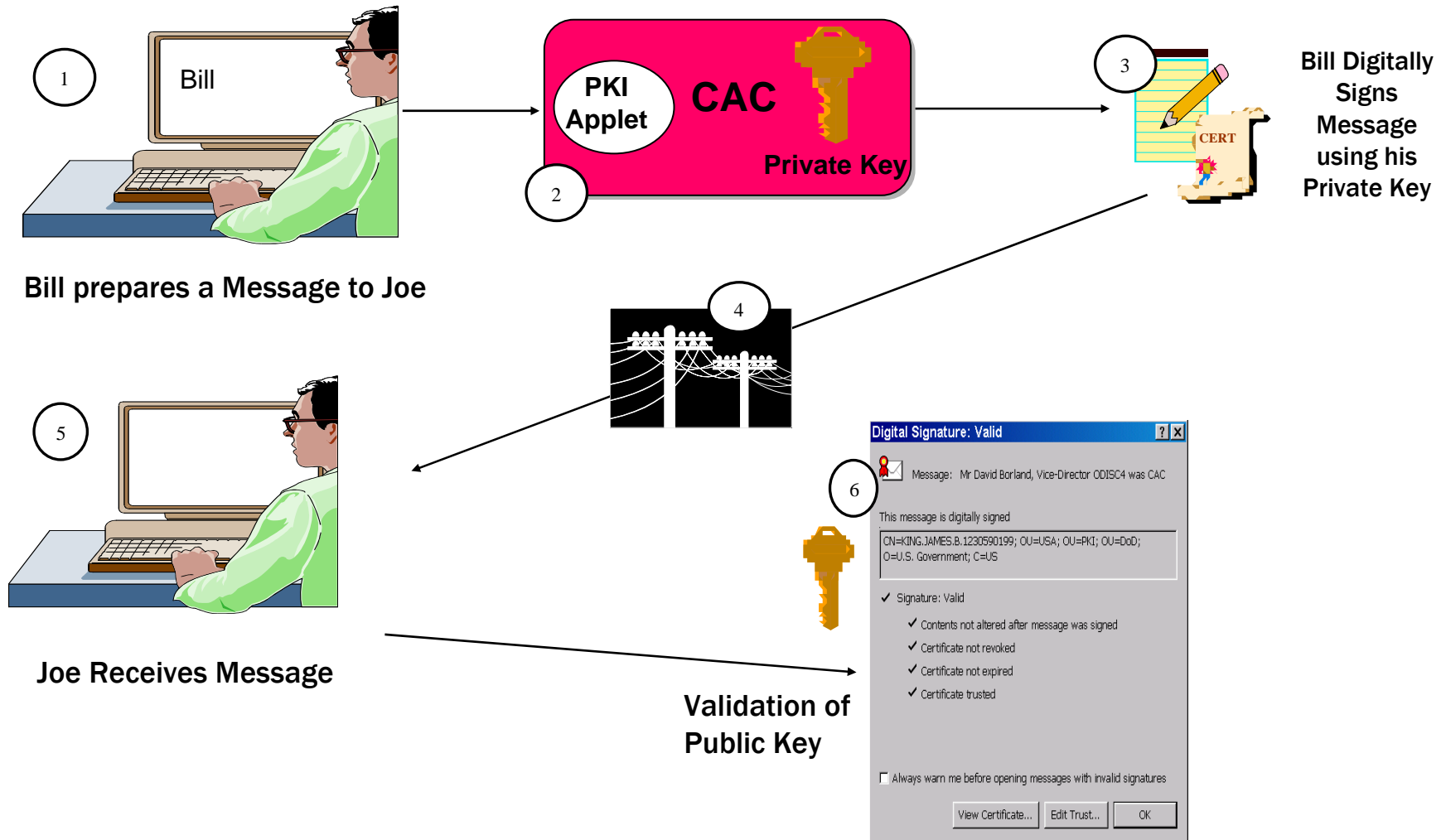
Security Requirements Solution



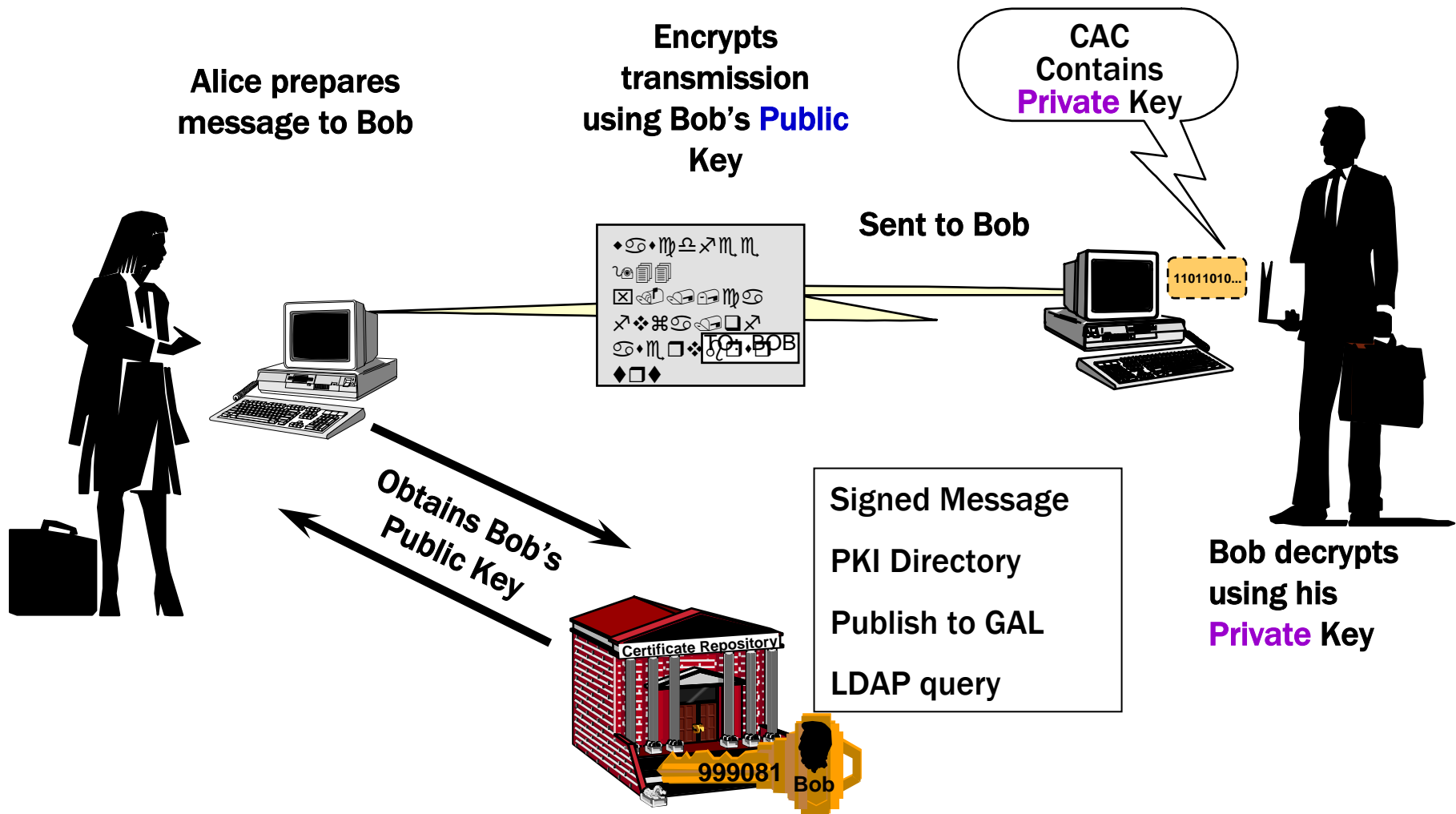
Signing and encrypting email meets 4 of the 7 Security Requirements

Security Requirements	Security Requirements Definition	Digital Signature	Encryption
Identification & Authentication	Assures that a person or system is exactly who or what they claim to be.		
Access Control	Provides access to authorized users while denying access to unauthorized users. (Provided by Identity Cert)		
Data Integrity	Protects against unauthorized changes in data whether they are intentional or accidental.		
Confidentiality	Protects against the disclosure of information to unauthorized users. Encryption is typically used to assure confidentiality when information is transmitted over networks.		
Non-Repudiation	Protects against a person denying later that a communication or transaction took place as recorded.		
Auditing	Monitors intentional or unintentional misuse of security features.		
Availability	Protects against loss of system operation as a result of malicious code, request flooding and penetration attempts		

Signing Email



Encrypting Email





End User Responsibilities

- **Protects their private key from disclosure.**
 - Your private key must be protected because anyone could use your digital signature or assume your digital identity.
 - It is your responsibility to ensure that no one gains access to your private key.
- **Reports any loss or compromise of his/her private key.**
 - It is presumed that only you have access to your private key. Should it be determined that someone else used your private key to sign a document, you may be liable for failing to adequately protect government property. If you suspect your PIN and private key are compromised, contact your ID issuance facility immediately.
- **Remember your PIN !**
 - If you forget your PIN, you will have to return to the ID issuance facility to have it reset.



Summary

- A Public Key Infrastructure ENABLES the use of
 - **Digital Signature**
 - **Encryption**
 - Which can be used to provide
 - » **Identification & Authentication**
 - » **Confidentiality**
 - » **Data Integrity**
 - » **Non-repudiation**
 - The Common Access Card is the hardware token that contains your private key.



Contact Information

Army Information Assurance CAC/PKI Helpdesk

Toll Free: 1-866-738-3222 (CONUS)

Local: 1-703-769-4499 (Washington Metro)

DSN 327-4004 (OCONUS)

Email: iacacpki.helpdesk@us.army.mil

Hours of Operation:

Monday - Friday 0730-1630

(7:30 AM to 4:30 PM Eastern Time)

DEERS/RAPIDS Site Locator: <http://www.dmdc.osd.mil/rs1>